Limitations on testing quantum theory

Fang Zhang\(^1\), Cupjin Huang\(^1\), Michael Newman\(^2\), Kevin Sung\(^1\) & Yaoyun Shi\(^1,3\)

\(^1\)Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48103, USA

\(^2\)Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

\(^3\)Alibaba Group, Bellevue, WA, USA

fangzh@umich.edu, cupjinh@umich.edu, mgnewman@umich.edu

kevjsung@umich.edu, y.shi@alibaba-inc.com

Abstract

How much of quantum theory can be experimentally tested? We investigate this question in an extreme scenario, when the experimenter cannot make any assumptions on the quantum description of a device or state. Instead, she can only directly manipulate and inspect classical information. We prove that in this scenario, there is almost nothing that she can ascertain about the internal state of a given quantum system. More precisely, for any initial state of a multi-partite system, there exists a different internal state so that any experiment performed on the system will produce identical statistics under these different states. In particular, we cannot certify if two subsystems are entangled. Our result implies that ascertaining the identity of a quantum state requires assumptions that cannot be experimentally tested through classical information alone.

Introduction

- Self-testing techniques allow one to certify the existence of entanglement between untrusted devices [2].

- Can we certify entanglement between untrusted states too?
  - Both store quantum information, but...
  - Untrusted devices can generate classical outputs on its own.
  - Untrusted states must be input into an untrusted device if we want to retrieve any information.

- If we simply input the states to the devices, we cannot determine whether the entanglement is between the input states or pre-existing between the devices themselves.

- Actually, there is no way to certify “anything interesting” about untrusted states.

- Adversarial implementations can make it so that all untrusted quantum states are in a maximally mixed joint state\(^4\).

Attacks

- In this work, an “attack” is defined as adversarial untrusted devices “simulating” other “honest” devices with identical classical behavior in a protocol.

- This work describes two “attacks”:
  - A “one-shot attack”, which only ensures that all quantum inputs to the protocol are in the maximally mixed state.
  - An extended attack, which also makes sure that all untrusted quantum states at any time point are in the maximally mixed state.

The One-Shot Attack

- Basic idea: encode all quantum inputs with a quantum secret sharing scheme [1].

  - Take an \((n, 2n − 1)\) threshold scheme (where \(n\) is the number of untrusted devices), put \(n − 1\) shares into the untrusted state, and allocate one share to each untrusted device.

  - Any one untrusted device plus the untrusted state can recover the original state.

  - All untrusted devices together can recover the original state even without the untrusted state.

Extension of the Attack

- Encode the outputs from the untrusted devices as well as the original input.

  - The devices cannot communicate directly with each other, but they can teleport some states nonetheless.

  - Some classical information is necessary to complete the teleportations...

  - Just bundle them with the untrusted state! They looks just like random strings!

Conclusions

- In theory, there are multiple possible “interpretations” of the world that are all consistent with quantum mechanics, but disagree on the quantum states.

  - For device-independent protocols, one has to be content with classical outputs unless other assumptions are added (such as trusted input states, or trusted but noisy devices).

  - The classical outputs (which we can read) are not affected: this attack is so “perfect” that it will do the correct thing even with the wrong quantum states!

References
